# Eine emanzipatorische Sicherheitskultur

**Dies ist der Einleitungsartikel einer Artikelserie zum Thema Kommunikationssicherheit in antiautoritären politischen Zusammenhängen. Wir veröffentlichen die Beiträge jeweils in der Zeitschrift Gai Dao und auf unserem Blog www.it-kollektiv.com.**
**Das IT-Kollektiv ist föderiertes Mitglied der FdA und Teil des Community-Projektes „IT-Kollektiv-Netzwerk“, das Kollektivbetrieben und Einzelpersonen aus dem IT-Bereich eine Plattform zur wirtschaftlichen und politischen Selbstorganisation bietet.**

★ *Von: IT-Kollektiv*

In den vergangenen Jahren ist IT-Sicherheit zu einem recht prominenten Thema im Diskurs des öffentlichen Mainstreams geworden. Zum Einen wird journalistisch über Sicherheitslücken in Software, spektakuläre Hackerangriffe und Geheimdienstaktivitäten berichtet. Zum Anderen treten zahlreiche NGOs und IT-Konzerne mit Ratgebern und Ähnlichem in Erscheinung. Offenbar fehlt es nicht an Inhalten zu diesem Thema. Warum also weitere Texte schreiben?




Trotz der Präsenz des Themas, konnte sich weder im persönlichen Technikgebrauch (#medienkompetenz) noch im aktivistischen Umfeld eine „Good Practice“ etablieren. Scheinbar haben die zum Teil konträren Beiträge nicht zur Aufklärung, sondern eher zu einer Abwendung vom Diskurs geführt. Eine Abwendung, die sich einerseits im „alles Egal“ der Post-Privacy-Gefärbten manifestiert, die spät Facebook und Co. für sich entdeckt haben und andererseits in Zusammenhängen, die die neuen Technologien komplett verdammen und sich in eigene Kommunikationsblasen zurückziehen.

Der permanente Nachrichtenstrom über Schwachstellen und neue Tools scheint den Blick auf etwas verbaut zu haben, das uns allen als Community einen Zugang zum Diskurs und eine Praxis liefern kann: Eine umfassende Sicherheitskultur. Bevor also technische Bausteine verschiedener Zielgruppen eine Rolle spielen können, gilt es, einen kulturellen Raum abzustecken. Dieser Ansatz entspricht unser horizontalen, antiautoritären Organisation und steht im Kontrast zu konventionellen Konzepten von Kontrolle, Überwachung, standardisierten Prozessen und Entscheidungswegen.

Zunächst stellt sich die Frage, was eine Sicherheitskultur leisten muss:

1. Sie soll uns vor Repression und Angriffen politischer Gegner*innen und wirtschaftlicher Ausbeuter*innen schützen.
2. Sie soll uns vor einer Steuerung unseres Denkens und Handelns durch Algorithmen und sogenannte „KIs“ schützen
3. Sie darf nicht zu einer Hierarchisierung unserer Strukturen führen.
4. Sie darf unsere Organisation nicht intransparent und unzugänglich machen.
5. Sie darf uns nicht aus politischen Prozessen isolieren.
6. Sie darf Beteiligte nicht anhand ihres technischen Know-Hows selektieren.

Für einen anarchistischen Zusammenhang erklären sich diese Anforderungen von selbst, eventuell ließen sie sich noch erweitern. Bei näherer Betrachtung oder spätestens bei der praktischen Umsetzung fällt auf, dass die Punkte 1+2 den Punkten 3-6 zuwider laufen. Dies liegt zum Einen im grundsätzlichen Widerspruch zwischen Transparenz und Teilhabe auf der einen und der Beschränkung des Kreises der Mitwissenden auf der anderen Seite. Zum Glück unterscheidet sich das für politische Teilhabe benötigte Wissen von jenem für Repression relevanten. Wenn Beispielsweise in einem

Protest ein Baugerät besetzt wurde, ist es wichtig den Raum zu schaffen Sinn und Durchführung dieser Aktion zu reflektieren. Das Wissen darüber, wer das Ganze wie durchgeführt hat, ist dagegen für die politische Teilhabe unerheblich.
Zum Anderen tragen eine Vielzahl existierender technischer Sicherheitsmaßnahmen eine autoritäre oder auch kapitalistische Ideologie in sich. Dies zeigt sich in der Vielzahl zentraler Sicherheits- und Genehmigungssysteme organisatorischer wie technischer Natur. Das kapitalistische Element manifestiert sich im Konkurrenzkampf um den Markt des Sicherheitsbedürfnisses. Abwechselnd wird Hysterie vor "Cybercrime" verbreitet und zahlreiche meist zweifelhafte Produkte angeboten. Wir sollen etwa auf unseren Geräten allerhand Software installieren oder unsere Passwörter in eine "sichere" Cloud laden, damit IT-Konzerne uns "schützen" können.
Erst in den letzten Jahren wurde der Punkt 2 relevant. Traditionell stützte sich staatliche Herrschaft und die Sicherung privatwirtschaftlicher Privilegien auf eine Kontrolle wichtiger Großmedien. Dies gilt für autoritäre Regime ebenso wie für Demokratien und lässt sich gerade in den Großwetterlagen der Außenpolitik beeindruckend mitverfolgen, liegt aber außerhalb des Fokus dieses Artikels. Durch die Entwicklung der sozialen Netzwerke sind die Prozesse der Meinungsbildung zeitweise entglitten. Seither wird die Kontrolle durch automatisierte Systeme in diesem Bereich wieder stärker ausgebaut. Dabei geht es nicht wie früher in erster Linie um Zensur und Veröffentlichungsverbote, sondern Algorithmen, die Informationen über Timelines, Vorschläge, verwandte Inhalte etc. verbreiten oder eben filtern. Die Funktionsweise dieser Algorithmen ist selten transparent. Dem*der Benutzer*in wird der Vorteil suggeriert genau die Inhalte zu bekommen, die sie interessieren. Unternehmen nutzen von Benutzer*innen erstellte Profile für Marketingzwecke und Dritte können öffentliche Sichtbarkeit erkaufen. Für die Steuerung unseres Denkens mittels Algorithmen müssen diese einerseits Kenntnis über unsere verschiedensten Daten erlangen und andererseits müssen wir deren Angebote nutzen.
Um sich den genannten Anforderungen zu nähern, will ich einige Thesen aufstellen und erläutern. Diese wären ein erster Vorschlag, der sich über die Artikelserie und eure Diskussionen vor Ort und Rückmeldungen weiter ausbauen ließe.

**Thesen:**

***1. Es gibt keine absolute Sicherheit***

Empfehlungen zu Sicherheit sind oft schon deshalb problematisch, weil sie nicht berücksichtigen vor welchen Angriffsszenarien sie eigentlich schützen sollen und den Schutzbedarf des zu sichernden Gegenstandes nicht bewerten. Daher gibt es keine absolute Sicherheit, sondern lediglich einer angemessenen Risikobewertung folgende Schutzmaßnahmen. Eine auf absolute Sicherheit zielende Vorgehensweise stellt letztendlich den zu sichernden Gegenstand als verbleibendes Risiko selbst in Frage. Absolute Sicherheit in der IT ist Funkstille.

***2. Wer Sicherheit will, muss sich fragen wovor***

Die Schutzmaßnahmen sehen im Allgemeinen grundsätzlich, je nach Angreifer*in und Angriffsszenario, verschieden aus. Wird bevorzugt Schutz vor unabhängigen Hacker*innen, anderen politischen Gruppen oder „Schurkenstaaten“ im Sinne der westlichen Auffassung gesucht, sind unter Umständen die großen IT-Konzerne und deren Angebote eine gute Grundlage für Sicherheit. Geht es allerdings darum, sich vor deren Datenhunger oder staatlichen Angriffen zu schützen, ist die Nutzung dieser Angebote ein großes Risiko. Da hilft dann auch kein 100-stelliges Passwort und Zwei-Faktor-Authentifizierung am Google-Konto.
Weiterhin besitzt jede*r Akteur*in eine Vielzahl verschiedener Angriffstechniken, die je einzeln zu erkennen und zu untersuchen sind.

***3. Es geht immer um Vertrauen***

Das Leben in Gemeinschaft genau wie politische Arbeit funktioniert nicht ohne Vertrauen und es gibt keine Sicherheitskultur, die ohne Vertrauen leben kann. Um so wichtiger ist es, offen zu legen, wem wir in Bezug auf was Vertrauen entgegenbringen. Bei IT wird diese Fragestellung leider sehr komplex. Da in unseren Zusammenhängen nur einige über das Know-How verfügen technische Systeme zu pflegen, vertrauen wir ihnen zumindest Meta-Daten und Verfügbarkeit von Infrastruktur an. Bei den heute gebräuchlichen Technologien allerdings meist auch Einsicht und Ver-

änderbarkeit der Inhalte. Wenn wir diese Tätigkeiten Menschen, die wir kennen, anvertrauen ist dies an sich kein Problem. Zum Schutz von uns und eben auch diesen Administrator*innen müssen wir uns dies aber vor Augen führen und entsprechend handeln.
In der IT Praxis ist leider der Kreis der „Vertrauten“ kaum mehr überschaubar (weshalb sich für manche Dinge allgemein die IT-Nutzung nicht empfiehlt). Durch Nutzung von Cloud-Diensten vertrauen wir ggf. IT-Großkonzernen und deren Mitarbeiter*innen die Kontrolle über unsere Daten an. Diese Nutzung ist bei Smartphones ab Werk überhaupt nicht mehr abstellbar. Wir vertrauen den Programmierer*innen von Software (bei Open Source Software und Freier Software zumindest kontrolliert durch eine Tech-Community). Wir vertrauen den Paket-Betreuer*innen, die aus Quellcode Maschinencode generieren. Wir vertrauen der hierarchischen Struktur der SSL-Zertifizierungs-Autoritäten und dem System der Namensauflösung des Internets. Die Liste lässt sich fortführen. Je nach Schutzbedarf lässt sich der Kreis der Vertrauten zumindest eindämmen und gezielt selektieren. Häufig vergessen wird dabei, dass zusätzlich zu den technischen auch organisatorische Maßnahmen gehören. Etwa die breite Wissensweitergabe an Gefährt*innen zur Nutzung ihrer Endgeräte im politischen und persönlichen Kontext.

***4. Direkt vor vermittelt; föderiert vor zentralisiert***

In unserer Sicherheitskultur gilt der alte Grundsatz die Zahl der Beteiligten auf das nötige Maß beschränkt zu halten. Das hat Konsequenzen für die Nutzung von IT-Lösungen. Idealerweise interagieren unsere Endgeräte direkt miteinander (Peer-2-Peer) ohne Beteiligung Dritter zur Datenvermittlung und Zertifizierung. Wir brauchen keine Server und keine „allmächtigen“ Administrator*innen. Dieser Ansatz ist jedoch nicht immer der Ideale, da er Probleme mit sich bringt. Einmal wird die Mandatierung von technischen „Expert*innen“ dadurch nicht überflüssig (was riskant wäre), weil die Absicherung der Endgeräte eher noch wichtiger wird und mehr Software auf den Clients installiert, gepflegt und aktuell gehalten werden muss. Technisch besteht bei Peer-2-Peer Netzwerken das Problem der Datenintegrität. Durch die nicht dauerhaft verfügbaren Einzelknoten bestehen Synchronisationsprobleme, d.h. der Verbindungsaufbau zwischen den Knoten scheitert und es kann keine Kommunikation stattfinden.




Wenn wir uns daher für einen vermittelten Ansatz entscheiden, sollten wir dezentralen (ggf. föderierten) Systemen den Vorzug geben. Dadurch können wir die Administration Vertrauten unserer Wahl überlassen und diesen ggf. auch das Mandat entziehen. Außerdem sind dezentrale Systeme weniger Angriffen ausgesetzt und potentiell verfügbarer. So kann beispielsweise der Staat den Server eines zentralisierten Messengers wie Signal oder einer Plattform wie linksunten Indymedia problemlos offline nehmen[1]. Würde er jedoch einen Mail-Anbieter wie Posteo plötzlich verbieten, könnten wir (wenn auch nicht über Posteo) weiterhin Emails versenden.

***5. Sicherheit ist ganzheitlich und so stark wie ihr schwächstes Element***

Zum einen tritt IT-Sicherheit oft so sehr in den Vordergrund, dass klassisches Sicherheitsdenken vernachlässigt wird. Nach wie vor werden Informant*innen eingesetzt, Räume abgehört, observiert und herumliegende Zettel gelesen. Zum Anderen wird beim Fokus auf eine Maßnahme vergessen, dass diese eventuell anders leicht umgangen werden kann. So kann sich leichtfertig etwa auf die starke Kryptografie eines Messengers verlassen werden ohne sich bewusst zu

sein, dass das Endgerät eines*einer Nutzer*in leicht angreifbar ist oder deren Identität nicht gesichert ist.

### 6. Die Sicherheitskultur umfasst unser ganzes Leben

Sicherheitskultur hat nicht nur mit Computern zu tun. Sie dreht sich auch nicht nur um politische Aktivitäten, sondern umfasst unser ganzes Leben und entsprechend muss es sich mit ihr auch leben lassen. Natürlich will manche*r allerhand Spaß mit Technik haben, aber dabei ist dann eben auf die Nutzung verschiedener Geräte oder virtueller Umgebungen und Identitäten zu achten. Auch sollte das persönliche Leben der Einzelnen eine Rolle in politischen Organisationen spielen und der Umgang sozialen Konformitätsdruck und Tabus reduzieren. Bekanntlich wird die Vereinzelung von uns immer wieder als Druckmittel verwendet. Psychische und finanzielle Notlagen können ausgenutzt werden oder wir können mit evtl. Suchtproblemen oder sexuell nicht normativem Verhalten erpresst werden.

### 7. Sicherheit ist nicht nur Geheimhaltung

Oft wird Sicherheit mit Geheimhaltung von Informationen gleichgesetzt. Allerdings besteht der Wert des zu schützenden Gegenstandes eben nicht nur aus deren informativem Gehalt, sondern auch aus dessen Nutz- und damit Verfügbarkeit. Er muss daher nicht nur vor Zugriffen geschützt werden sondern im Gegenteil muss die legitime Zugreif- und Nutzbarkeit sichergestellt werden. Verschiedene Angriffe zielen genau hierauf. Etwa Denial-of-Service-Attacken, das behördliche Sperren von Diensten oder ganz klassisch das Verbot von Versammlungen oder Veröffentlichungen.

### 8. Unsere Entscheidungen zu Sicherheitskultur sollen nicht anderen verunmöglichen, ihre Sicherheitskultur zu leben

Wir können uns entscheiden, unsere Termine auf Facebook zu veröffentlichen, um viele Menschen zu erreichen, obwohl es potentiell offenlegt, wer unsere Veranstaltungen besucht. Oder wir können Twitter benutzen, um über unsere Aktion zu informieren. Falls wir aber nicht gleichzeitig andere mögliche Kanäle nutzen, wie die Stadtteilzeitung, einen online Terminkalender einer netten Gruppe oder ein freies Microbloggingmedium, dann zwingen wir Andere, Technologien zu nutzen, die wir (sicherheits-)politisch eigentlich ablehnen.

### 9. Sicherheit ist das Gegenteil von Paranoia

Paranoia ist ein Zustand der Lähmung Einzelner oder ganzer Zusammenhänge. Sie könnte als ein erfolgreicher Angriff auf unsere Strukturen bewertet werden. In der Paranoia fokussieren wir uns nicht mehr auf politische Ziele, sondern auf Geheimhaltung. Angst und Misstrauen verunmöglichen gemeinsame Organisierung oder eine sachliche Einschätzung unseres Handelns. ■

**Endnote**:
[1] Dies kann auf technischem Wege erfolgen wie im Falle Telegram im Iran oder mittels rechtlicher Repressionsandrohungen wie im Falle Linksunten.
Quelle: https://www.theverge.com/2018/1/2/16841292/iran-telegram-block-encryption-protest-google-signal